

# Coats & Bennett

12-13-99

1100 Crescent Green  
Suite 206  
Cary, North Carolina 27511  
tel: 919-854-1844  
fax: 919-854-2084  
www.coatsandbennett.com

Patents, Trademarks,  
Copyrights, Trade Secrets,  
Licensing, and  
Related Litigation

Patent Attorney  
Larry L. Coats  
David E. Bennett  
Benjamin S. Withrow  
John R. Owen  
David D. Kallen  
Steven N. Terranova  
Taylor M. Davenport

Patent Agent  
Michael D. Murphy

December 10, 1999

**VIA EXPRESS MAIL LABEL NO. EL527475247US**  
**BOX PATENT APPLICATION**

Honorable Commissioner of Patents  
and Trademarks  
Washington, D.C. 20231

RE: U.S. Patent Application  
Inventors: Mohammad Peyravian, Allen Roginsky, Nevenko Zunic, and  
Stephen M. Matyas, Jr.

**TIME STAMPING METHOD USING TIME-BASED SIGNATURE**  
**KEY**

Dear Sir:

Enclosed please find the above-identified U.S. Patent Application, which includes the following:

1. Specification and Claims
2. Formal Drawings (3 sets of 1 sheet)
3. Declaration and Power of Attorney for Patent Application (unsigned)
4. Form PTO-1449 and Related Patents
5. Fee Transmittal Form
6. **Express Mail Certification - Label No. EL527475247US**
7. Postcard

Please deduct all fees associated with this application from IBM's Deposit Account No. 09/0461.

Respectfully submitted,

**COATS & BENNETT, P.L.L.C.**

By:

*David E. Bennett*

David E. Bennett  
Registration No. 32,194

DEB/jjr  
Enclosures  
P-4541.006

Jc518 U.S. PTO  
12/10/99

COATS & BENNETT

PTO  
12/10/99

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: )  
)  
Peyravian et al. )  
)  
Serial No. \_\_\_\_\_ )  
)  
Filed: \_\_\_\_\_ )  
)  
For: **TIME STAMPING METHOD** )  
**USING TIME-BASED** )  
**SIGNATURE KEY** )  
)  
Attorney's Docket No. P-4541.006 )

**Express Mail Certification**  
**Label No.EL527475247US**

Raleigh, North Carolina

December 10, 1999

Honorable Commissioner of Patents and Trademarks  
**BOX PATENT APPLICATION**  
Washington, D.C. 20231

Sir:

**EXPRESS MAIL CERTIFICATE LABEL NO. EL527475247US**

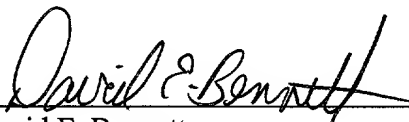
**DATE MAILED: December 10, 1999**

I hereby certify that the enclosed specification and claims, drawings (3 sets of 1 sheet), Declaration and Power Of Attorney (unsigned), Fee Transmittal form, form PTO-1449 and related patents, are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. §1.10 on the date indicated above and is addressed to Honorable Commissioner of Patents and Trademarks, BOX PATENT APPLICATION, Washington, D.C. 20231.

Respectfully submitted,

**COATS & BENNETT, P.L.L.C.**

By:

  
\_\_\_\_\_  
David E. Bennett  
Registration No. 32,194

Telephone: (919) 854-1844

# **UNITED STATES PATENT APPLICATION FOR GRANT OF LETTERS PATENT**

**MOHAMMAD PEYRAVIAN  
ALLEN ROGINSKY  
NEVENKO ZUNIC  
STEPHEN M. MATYAS, JR.  
INVENTORS**

COATS & BENNETT, P.L.L.C.

## **TIME STAMPING METHOD USING TIME-BASED SIGNATURE KEY**

**COATS & BENNETT, P.L.L.C.**

P.O. Box 5  
Raleigh, NC 27602  
(919) 854-1844

# **TIME STAMPING METHOD USING TIME-BASED SIGNATURE KEY**

## **BACKGROUND OF THE INVENTION**

The present invention relates generally to cryptographic protocols and, more particularly, to a time-stamping protocol for time-stamping digital documents.

There are times when it is desirable to prove the existence of a document as of a particular date. For example, patent disputes concerning the inventorship of an invention often turn on who is able to produce corroborating documentary evidence dating their conception of the invention. A common procedure for dating records is to keep the records in a daily journal or notebook with each page sequentially numbered and dated. Another procedure for dating a record is to have the record witnessed by an uninterested or trusted party that can attest to the existence of the document. The increasing use of computers, however, makes these time-stamping methods obsolete. It is relatively easy to change the date-stamp added to a document by the computer when the document was created. Further, while it is difficult to alter a paper document without leaving some signs of tampering, digital records can be easily altered or revised without leaving any evidence of tampering. Therefore, people are less likely to trust a digital document than a paper document that has been time-stamped using conventional time-stamping procedures.

To be trusted, a time-stamping procedure for digital documents should meet the following criteria:

1. The data itself must be time-stamped, without any regard to the physical medium on which it resides.
2. It must be impossible to change a single bit of the data without that change being apparent.
3. It must be impossible to timestamp a document with a date and time different than the current date and time.

One method for time-stamping a digital document would be to archive the document with a trusted escrow agent. In this case, the document originator sends a copy of the digital document to a trusted escrow agent. The escrow agent records the date and time that the document was received and retains a copy in his archives. Later, if a dispute arises over the date of the document, the document originator can contact the escrow agent who produces his copy of the document and verifies that it was received on a particular date. This time-stamping procedure has a number of drawbacks. First, the document originator must disclose the contents of the document to the escrow agent. Also, large documents take a relatively long period of time to transmit to the escrow agent and they require a large amount of data storage.

An improvement of the escrow procedure is to use a hash of the document. Instead of sending the document to the escrow agent, the document originator hashes the document using a one-way hash algorithm and sends the generated hash value to the escrow agent. The escrow agent stores the hash

value along with the date and time that it was received in his archives. Later the document originator can use the services of the escrow agent to prove the existence of the document as of a particular date. The disputed document can be hashed and the resulting hash value can be compared to the hash value stored by the escrow agent in his archives for equality. If the hash values are equal, the document is presumed to be in existence as of the date associated with the stored hash value. One advantage of this method is that the document originator does not need to disclose the contents of the document to the escrow agent.

The need to escrow the document or hash value can be eliminated by having a time stamping authority generate a certified time stamp receipt using a cryptographic signature scheme as taught in U.S. Pat. No. Re. 34,954 to Haber et al. and Fischer, U.S. Patent No. 5,001,752. In this case, the document originator hashes the document and transmits the hash value to the time stamping authority. The time stamping authority appends the current date and time to the hash value to create a time stamp receipt and digitally signs the time stamp receipt with a private signature key. The time stamping authority's public verification key is distributed and available to anyone interested in validating a time stamp receipt created by time stamping authority. The public verification key is typically stored in a public key certificate signed by a Certification Authority so that anyone desiring to validate the time stamp receipt with the public key can have confidence in the authenticity of the key.

Another approach to time stamping documents is disclosed in PCT WO 99/16209 entitled Method and System For Transient Key Digital Time Stamps. In this application, time stamp receipts are signed by the time stamping authority using transient, time-related keys. The time-stamping authority periodically generates a signature generation key, which is valid for a predetermined interval of time. Documents received during the specified time interval are signed using the key corresponding to that interval. At the end of the interval, a new key is generated for the next interval and the previously used key is discarded. In this manner, a new signature generation key is generated at a predetermined interval of time. The public verification key associated with each private signature generation key is saved for future authentication of the time stamp receipt.

## SUMMARY OF THE INVENTION

The present invention is a time-stamping protocol for time-stamping digital documents so that the date of the document can be verified. The method presumes the existence of a trusted agent referred to herein as the time-stamping authority (TSA). The TSA has a time-based signature key that the TSA uses to sign time stamp receipts. The signature key is associated with a fixed time reference. According to the present invention, a requestor sends a document to be certified or other identifying data associated with the document to a time-stamping authority TSA. The TSA creates a time stamp receipt by computing a time difference between the time reference associated with the signature key and the time the document was received. The time difference is

appended to the identifying data received by the TSA to create a time stamp receipt and the receipt is then signed by the TSA and transmitted to the requestor.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a flow diagram illustrating the time stamping method embodiment of the time stamping method of the present invention.

## DETAILED DESCRIPTION OF THE INVENTION

Figure 1 is a flow diagram illustrating the general process of time-stamping a document according to the present invention. A document D is created at step 100. The document D is presumed to be in digital form and may comprise any alphanumeric, audio, or graphic presentation of any length. The document D may optionally be hashed at step 102 using a one-way hashing function. A hash function is a function that takes a variable length input string, called a pre-image, and converts it to a fixed-length string, called a hash value, denoted H. The pre-image in this case is the document D or selected portions thereof. A one-way hash function operates in only one direction. While, it is easy to compute a hash value from the pre-image, it is computationally impractical to find a pre-image that hashes to a given hash value. Thus, it is practically impossible to recover the pre-image given the hash value and knowledge of the hash algorithm. Another feature of a hashing function is that it is difficult to find any two pre-images that hash to the same value.



There are several advantages to sending a hash value  $H$  produced on document  $D$  instead of the document  $D$  itself. First, the hash value  $H$  improves security by functioning as a fingerprint of the document  $D$ . Changing a single bit in the document  $D$  will result in an entirely different hash value making it easy to detect efforts to modify a document  $D$  or hash value  $H$ . Second, the hash value  $H$  greatly reduces the amount of data that must be transmitted to the TSA. This factor can be important where the available bandwidth is limited. Third, by sending a hash value  $H$  in place of the document  $D$ , the content of the document  $D$  does not need to be disclosed to the TSA.

Any known hashing function, such as the SHA-1, MD5, and RIPEMD-160, can be used in the present invention. For the remaining description of the time stamping protocol, it will be assumed that the document  $D$  has been hashed and that the hash value  $H$  has been sent to the TSA in lieu of the document  $D$ . It is understood, however, that one can practice the invention by substituting  $D$ , selected portions of document  $D$ , or some other function of  $D$  in place of the hash value  $H$  in the protocol.

The hash value  $H$  generated on document  $D$  or a selected portion thereof is transmitted to and received by the TSA at step 104 as part of a certification request. According to the present invention, the TSA has a time-based private signature key that the TSA uses to sign time stamp receipts  $R$ . The private signature key is part of a public and private key pair  $(K_P, K_{PR})$ . The private signature key  $K_{PR}$  is known only to the TSA. The public verification key  $K_P$  is made available to the public so that anyone can verify or authenticate the TSA's

signature. The public key  $K_P$  can be stored in a certificate signed by a Certification Authority CA so that the TSA's public key can be validated and, hence, trusted by those using the public verification key  $K_P$ . The key pair has an associated time reference  $T_{REF}$  that is stored in the public key certificate along with the public verification key  $K_P$ . The time reference  $T_{REF}$  in the public key certificate can be established by the TSA when requesting the public key certificate or may be determined by the Certification Authority, or some completely independent means.

At step 106, the TSA computes a time difference  $\Delta T$  between the time reference  $T_{REF}$  recorded in the public key certificate and the current time  $T$ . The current time  $T$  is generated by a trusted clock controlled by the TSA, or alternatively, is obtained by the TSA from a trusted source. The TSA creates a time stamp receipt  $R$  at step 108 using the computed time difference  $\Delta T$ . The time stamp receipt  $R$  is generated by concatenating the hash value  $H$  with the computed time difference  $\Delta T$  and optionally other data, such as the identification number  $ID$  of the requestor and a sequential record number  $SN$ . Requiring an identification number  $ID$  and sequential record number  $SN$  may improve security by making it more difficult to create counterfeit time stamp receipts. The time stamp receipt  $R$  would then comprise the string  $(H, \Delta T, ID, SN)$ . The TSA then signs the time stamp receipt at step 110 and transmits the time stamp receipt to the requestor at step 112. The signed time stamp is denoted  $\text{sig}(R)$ .

In the event that a dispute arises concerning document  $D$ , the existence and substance and the document  $D$  as of a particular date can be proved by

means of the signed time stamp receipt  $\text{sig}(R)$ . To verify the document  $D$ , the TSA's signature on the time stamp receipt,  $\text{sig}(R)$ , is first verified using the TSA's public verification key  $K_P$ . Next, the disputed document  $D$  is verified against the hash value  $H$  contained in the time stamp receipt  $R$ . A hash value  $H$  is generated on the disputed document  $D$  and compared for equality to the hash value  $H$  contained in the signed time stamp receipt  $\text{sig}(R)$ . The date or time of the document  $D$  is computed by adding the time difference  $\Delta T$  contained in the signed time stamp receipt  $\text{sig}(R)$  to the time reference  $T_{\text{REF}}$  taken from the public key certificate.

The time-stamping procedures described herein may be implemented using general purpose programmable computers. A client program running on a user's computer could perform the steps of hashing documents, generating time stamp receipts, and transmitting time stamp receipts to the TSA. A server application running on a general purpose programmable computer controlled by the TSA could perform the steps of validating time stamp receipts, signing time stamp receipts, generating certificates, and transmitting signed time stamp receipts to users. It would also be possible to implement some or all of the steps in firmware, or in hard-wired logic.

The present invention may, of course, be carried out in other specific ways than those herein set forth without departing from the spirit and essential characteristics of the invention. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive, and all changes

coming within the meaning and equivalency range of the appended claims are intended to be embraced therein.

Claims:

1. A method for time stamping a document comprising:
  - receiving identifying data associated with said document at an outside agency;
  - computing at said outside agency a time difference between a predetermined time reference and the time of receipt of said identifying data;
  - creating a time stamp receipt by associating said time difference with said identifying data; and
  - certifying said time stamp receipt by signing said time stamp receipt at said outside agency with a private signature key associated with said predetermined time reference.
2. The time stamping method of claim 1 further including transmitting said certified time stamp receipt to a designated party.
3. The time stamping method of claim 1 wherein said identifying data comprises a digital copy of at least a portion of said document.
4. The time stamping method of claim 3 wherein said identifying data comprises a digital representation of said document derived by application of a deterministic function to at least a portion of said document.

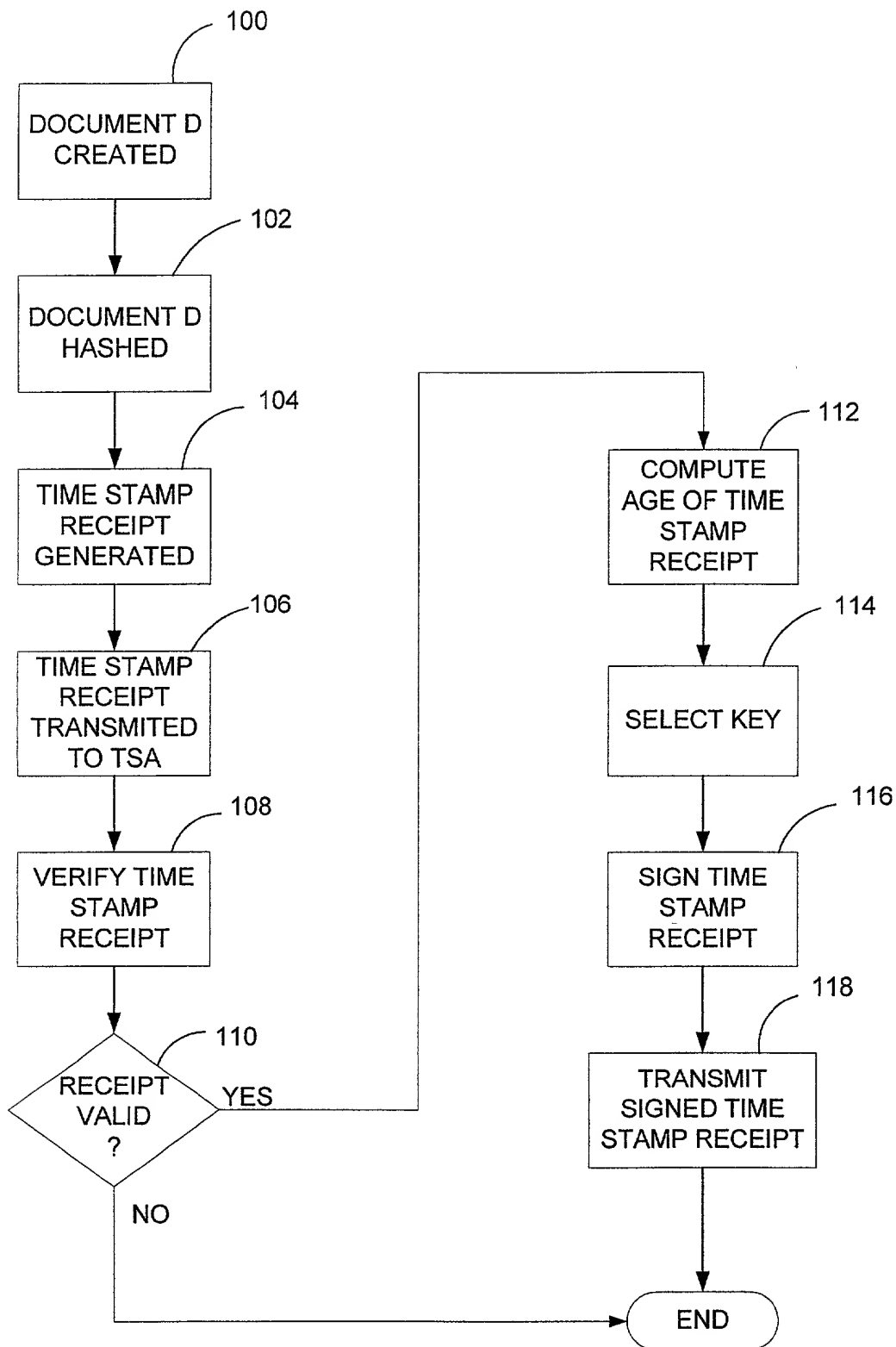
5. The time stamping method of claim 4 wherein said digital representation is a hash value derived by application of a one-way hashing function to at least a portion of said document.
6. The time stamping method of claim 1 wherein said time stamp receipt includes a copy of at least a portion of said identifying data concatenated with said time difference.
7. The time stamping method of claim 6 wherein said time stamp receipt includes a digital sequence derived from said identifying data concatenated with said time difference.
8. The time stamping method of claim 1 wherein said time stamp receipt further includes an identification number associated with the document originator.
9. The time stamping method of claim 8 wherein said time stamp receipt further includes a sequential record number.
10. The time stamping method of claim 1 wherein said time reference is stored in a public key certificate.
11. The time stamping method of claim 1 wherein the step of certifying said time stamp receipt includes encrypting said time stamp receipt using a private

signature key controlled by said outside agency, wherein said time stamp receipt can be later verified by decrypting the signed time stamp receipt with a corresponding public verification key.

## ABSTRACT OF THE DISCLOSURE

A time-stamping protocol for time-stamping digital documents uses a time-based signature key. A document or other identifying data is sent to a time stamping authority TSA. The TSA has a time-based signature key that the TSA uses to sign time stamp receipts. The signature key is associated with a fixed time reference that is stored in a public key certificate also containing the public verification key. Upon receiving the document, the TSA creates a time stamp receipt by computing a time difference between the time reference associated with the signature key and the time the document was received. The time difference is appended to the document to create a time stamp receipt and the receipt is then signed by the TSA and transmitted to the requestor.





**FIG. 1**

### Declaration and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

#### TIME STAMPING METHOD USING TIME-BASED SIGNATURE KEY

the specification of which (check one)

☒

is attached hereto.

☐

was filed on \_\_\_\_\_ as Application Serial No. \_\_\_\_\_.

I hereby state that I have reviewed and understand the contents of the above- identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):			
Number	Country	Day/Month/Year	Priority Claimed

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U.S. Applications:		
Serial No.	Filing Date	Status

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

A.B. Clay, Reg. No. 32,121; G. M. Doudnikoff, Reg. No. 32,847; E. H. Duffield, Reg. No. 25,970; J. W. Herndon, Reg. No. 27,901; J. S. Ray-Yarletts, Reg. No. 39,808; Larry L. Coats, Reg. No. 25,620, David E. Bennett, Reg. No. 32,194; John R. Owen, Reg. No. 42,055; Benjamin S. Withrow, Reg. No. 40,876; David D. Kalish, Reg. No. 42,706; Steve Terranova, Reg. No. 43,185; Taylor M. Davenport, Reg. No. 42,466; and Michael D. Murphy, Reg. No. 44,958.

Send all correspondence to:

IBM Corporation, Dept. T81/062  
3039 Cornwallis Road  
RTP, NC 27709  
919-543-2541  
FAX: 919-254-4330

---

(1) Inventor: Mohammad Peyravian

Signature: \_\_\_\_\_ Date \_\_\_\_\_

Residence: Cary, North Carolina, USA

Citizenship: US

Post Office Address: 122 Lake Hollow Circle, Cary, North Carolina 27513

(2) Inventor: Allen Roginsky

Signature: \_\_\_\_\_ Date \_\_\_\_\_

Residence: Durham, North Carolina, USA

Citizenship: US

Post Office Address: 5610 Loyal Avenue, Durham, North Carolina 27713

(3) Inventor: Nevenko Zunic

Signature: \_\_\_\_\_ Date \_\_\_\_\_

Residence: Wappingers Falls, New York, USA

Citizenship: US

Post Office Address: 45 Reggie Drive, Wappingers Falls, New York 12590

(4) Inventor: Stephen M. Matyas, Jr.

Signature: \_\_\_\_\_ Date \_\_\_\_\_

Residence: Manassas, Virginia, USA

Citizenship: US

Post Office Address: 10298 Cedar Ridge Drive, Manassas, Virginia 20110